AMENDMENTS TO THE CLAIMS

The following is a complete, marked-up listing of revised claims with a status identifier in parenthesis, underlined text indicating insertions, and strike through and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS

1. (Currently Amended) ~~Authentication~~ An authentication method of at least one application working in an equipment connected by a network to a control server, said equipment being locally connected to a security module, said application being at least one of loadable and executable via an application execution environment of the equipment and said application being adapted to use resources stored in the security module, the method comprising:

receiving by the control server, via the network, identification data ~~comprising~~ including at least an identifier of the equipment and ~~the identifier of~~ an identifier of the security module,

analyzing and verifying, by the control server, said ~~the~~ identification data,

generating, by the control server, a cryptogram ~~comprising~~, the cryptogram including a digest of the application, the identification data and instructions intended for the security module,

transmitting the application and the cryptogram by the control server, via the network and the equipment, to the security module, and

verifying, by the security module, the application by comparing the digest extracted from the received cryptogram with a digest determined by the security module,

wherein, during at least one of initialization and activation of the application, the security module executes the instructions extracted from the cryptogram and, according to a result of the verification of the application,

performs at least one of ~~releases~~ releasing and ~~blocks~~ blocking access ~~to~~ of certain resources of said security module to the application~~according to a result of the verification specific to the application previously obtained~~.

2. (Currently Amended) ~~Method~~ The method according to claim 1~~wherein~~, wherein the equipment is a mobile equipment of mobile telephony.

3. (Currently Amended) ~~Method~~ The method according to claim 1~~wherein~~, wherein the network is a mobile network of at least one of ~~the type~~a GSM, GPRS, and UMTS.

4. (Currently Amended) ~~Method~~ The method according to ~~claim 1~~claim 2, wherein the security module is a subscriber identification module that is inserted into the mobile equipment of mobile telephony~~of a SIM card type~~.

5. (Currently Amended) ~~Method~~ The method according to claim 4~~wherein~~, wherein the identification data of at least one of the ~~set~~ mobile equipment and subscriber identification module ~~comprises~~ includes an identifier of the mobile equipment and an identifier of the subscriber identification module pertaining to a subscriber ~~to~~ of the network.

6. (Currently Amended) ~~Method~~ The method according to claim 1~~wherein~~, wherein the instructions included in the cryptogram received by the security module condition the use of the ~~applications~~ application according to criteria established previously by at least one of the operator, the application supplier and the user of the equipment.

7. (Currently Amended) ~~Method~~ The method according to claim ~~6 wherein,~~ wherein the criteria define limits of use of the application according to risks associated with at least one of the software of the application and ~~with~~ the hardware of the equipment that the operator desires to take into account.

8. (Currently Amended) ~~Method~~ The method according to claim 1 ~~wherein,~~ wherein the verification of the application with the cryptogram is carried out at the time of at least one of the first initialization and the first use of the application.

9. (Currently Amended) ~~Method~~ The method according to claim 1 ~~wherein,~~ wherein the verification of the application with the cryptogram is periodically carried out at a given rate according to instructions originating from the control server.

10. (Currently Amended) ~~Method~~ The method according to claim 1 ~~wherein,~~ wherein the verification of the application with the cryptogram is carried out at the time of each initialization of said application on the equipment.

11. (Currently Amended) ~~Method~~ The method according to claim 1 ~~wherein,~~ wherein the cryptogram is generated with the aid of an asymmetrical or symmetrical encryption key from a data set ~~containing, among other data,~~ including the identifier of the equipment, the identifier of the security module, an identifier of the application, the digest of the application calculated with an unidirectional hash function, identifiers of the resources of the security module and instructions for blocking or releasing resources of the security module.

12. (Currently Amended) ~~Method~~ The method according to claim 11 ~~wherein~~, wherein the cryptogram includes a variable that is predictable by the security module thereby avoiding the double use of a same cryptogram, the value of said variable ~~being~~ controlled by the security module by comparing the value of the variable ~~making a comparison with that of~~with a reference value, the reference value being stored in the security module and regularly updated.

13. (Currently Amended) ~~Method~~ The method according to claim 1 ~~wherein~~, wherein the security module transmits to the control server, via the equipment and the network, a confirmation message when the security module has accepted or refused a cryptogram of an application.

14. (Currently Amended) ~~Method~~ The method according to the claim 1 ~~wherein~~, wherein the cryptogram is transmitted to the security module at the same time as the application is loaded into the equipment via the application execution environment ~~of the applications~~.

15. (Currently Amended) ~~Method~~ The method according to claim 1 ~~wherein~~, wherein the application, once loaded into the equipment from the control server via the network, requests a cryptogram from the server at the time of its initialization and transmits said cryptogram to the security module, the confirmation message of acceptance or refusal of the cryptogram being transmitted by the security module to the server via the application.

16. (Currently Amended) ~~Method~~ The method according to claim 1, wherein the equipment is at least one of a Pay-TV decoder ~~or~~ and a computer to which the security module is connected.

17. (Currently Amended) ~~Security~~ A security module comprising resources intended to be accessed locally by at least one application installed in an equipment connected to a network,

said equipment including means for reading and transmitting data, the transmitted data including at least one of an identifier of the equipment and an identifier of the security module, said security module further ~~comprising~~ including means for reception, storage and analysis of a cryptogram and of the at least one application received with the cryptogram,

wherein the cryptogram includes ~~containing among other data,~~ a digest of said application and instructions, means for verification of said at least one application, and means for extraction and execution of the instructions contained in the ~~cryptogram,~~cryptogram, the means for extraction and execution performing ~~for~~ at least one of releasing and blocking certain resources of the security module to the at least one application according to ~~the~~ a result of the verification of the at least one application.

18. (Currently Amended) ~~Security~~ The security module according to claim 17, wherein the security module is ~~at least one of the~~ a subscriber identification module ~~and SIM card type intended to be~~that is connected to a mobile equipment.

19. (Currently Amended) ~~Method~~ The method according to claim 2, wherein the security module is a subscriber identification module that is inserted into the mobile equipment of mobile telephony ~~of the SIM card type~~.

*** END CLAIM LISTING ***